



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/596,003	02/08/2007	Maria Pilar Gonzalez Lopez	PI8126-US1	1612
27045	7590	12/13/2010		
ERICSSON INC.			EXAMINER	
6300 LEGACY DRIVE			KATSIKIS, KOSTAS J	
M/S EVR 1-C-11				
PLANO, TX 75024			ART UNIT	PAPER NUMBER
			2441	
NOTIFICATION DATE	DELIVERY MODE			
12/13/2010	ELECTRONIC			

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

kara.coffman@ericsson.com  
jennifer.hardin@ericsson.com  
melissa.rhea@ericsson.com

<b>Office Action Summary</b>	<b>Application No.</b> 10/596,003	<b>Applicant(s)</b> GONZALEZ LOPEZ ET AL.
	<b>Examiner</b> Kostas Katsikis	<b>Art Unit</b> 2441

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If no period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 20 September 2010.

2a) This action is FINAL.      2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 37-72 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 37-72 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date \_\_\_\_\_

5) Notice of Informal Patent Application  
 6) Other: \_\_\_\_\_

**DETAILED ACTION**

1. This communication is in response to Amendment filed September 20, 2010, in which claims 37, 51, and 62 have been amended. Accordingly, claims 37-72 remain pending for examination.

**Status of Claims**

2. Claims 37-72 are pending, of which claims 37-72 are rejected under 35 U.S.C. 102(b).

3. **Examiner's Note:** Examiner has cited particular paragraphs and/or columns and line numbers in the references applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. **Claims 37-72 are rejected under 35 U.S.C. 103(a) as being anticipated over Barker et al. (United States Patent No. US 6,363,421 B2), hereinafter “Barker”.**

Regarding claims 37, 51, and 62, Barker discloses an hardware-containing apparatus for mediating in management orders between a plurality of origin managing devices and a plurality of managed devices in a telecommunications system, the management orders intended to execute management operations over the managed devices, comprising (*wherein a plurality of network elements of a telecommunication network is managed through an element management system server coupled through a communication link including the computer internet to a management computer*)  
**(Barker, Abstract):**

a communication receiver component arranged to receive a management order from one of the origin managing devices (*wherein the interface of the element management system server 32 receives management commands from the client 28 of the management computer 26 for the management of the application processor*

**80/network element 14) (Barker, FIG. 1A-1C, and FIG. 2-4 combined, col. 1, line 25-col. 2, line 33);**

a management verifier component arranged to determine whether the received management order is an allowed management order by checking whether the management order fits an access attribute comprised in a management access template, the management access template being one selected from the group consisting of (*wherein upon startup, client of management computer registers with the server by providing identification of the client host, port, client, and a password. The server retrieves the client record from local data services and returns a session object to the client noting the client's access permissions. This information may be used to provide some level of access control in the client application (e.g. deactivating menu element management system for maintenance operations that are not allowed). All requests are validated at element management system server*) (Barker, col. 30, lines 45-63); a first management access template in relationship with an identifier of the origin manager (*wherein management information base (MIB) stores object attributes related to a registered management computer 26/application processor 80. Client applications utilize the EMAPI 55 to access service objects on the server which provide access to attributes of the managed objects, provide maintenance operations for those managed objects, and allow the client to register for notifications of attribute changes and event notifications*) (Barker, FIG. 3 and FIG. 4 combined, col. 7, lines 45-63, col. 10, line 50-col. 11, line 60); a second management access template in relationship with an identifier of a managed data object affected by the management order (*wherein*

*management information base (MIB) stores object attributes referenced by specific object class IDs and attribute codes) (Barker, FIG. 3 and FIG. 4 combined, col.13, line 45-col. 14, line 60); and a third management access template in relationship with an identifier of a managed device affected by the management order (wherein management information base (MIB) stores object attributes related to network element. Each object that represents a network element or maintenance unit in a network element utilizing SNMP for its protocol (e.g. AP, DS1, EIN, LAN) is represented as a "SnmpMO" class object 170) (Barker, FIG. 3 and FIG. 4 combined, col. 11, lines 47-60); and*

a communication sender component arranged to send an allowed management order to a managed device (wherein HPOV processes 70/CMU SNMP library relay management commands to network element 14) (Barker, FIG. 3 and FIG. 4 combined, col. 5, lines 24-48, col. 7, line 45-col. 8, line 7);

the hardware-containing apparatus is interposed between the plurality of origin managing devices and the plurality of managed devices so as to receive management orders from the plurality of origin managing devices and issue allowed management orders to the plurality of managed devices (wherein element management system server 32 is between network element 14 and management computer 26 for relaying SNMP management commands) (Barker, Abstract, FIG. 1-4, col. 1, line 25-col. 2, line 33).

Claim 62 includes a computer program for performing the limitations substantially as described in claim 37. Barker discloses a computer program for mediating from a

Art Unit: 2441

computer-based apparatus in management orders between a plurality of origin managers and a plurality of managed devices in a telecommunications system for performing the limitations substantially as described in claim 37 (*wherein element management system server in telecommunications network comprises storage with plurality of software components*) (**Barker, FIG. 3 and FIG. 4 combined, col. 5, line 24-col. 6, line 52, col. 8, lines 1-28**). The motivation regarding the obviousness of claim 37 is also applied to claim 62; therefore, claim 62 is rejected under the same rationale.

Additionally, claim 51 recites a method for mediating in the management of a plurality of devices from a plurality of origin managers that performs the limitations substantially as described in claims 37 and 62 and is rejected for similar reasons.

Regarding claim 38, **Barker** discloses the apparatus of claim 37, wherein the first management access template further comprises at least one access attribute selected from the group consisting of: an identifier of an allowed management operation (*wherein Each managed object class requires the session identifier as a parameter to each public method. The access permissions associated with the session are examined before authorizing client execution*) (**Barker, col. 30, lines 56-60**); an identifier of an allowed managed data object; a pattern structure of the managed data object; an identifier of an allowed managed device; an identifier of an allowed management operation over an allowed managed device; and an identifier of an allowed management operation over an allowed managed data object.

Regarding claim 39, **Barker** discloses the apparatus of claim 37, wherein the second management access template further comprises at least one access attribute selected from the group consisting of: a pattern structure of the managed data object; an identifier of an allowed management operation (*wherein Each managed object class requires the session identifier as a parameter to each public method. The access permissions associated with the session are examined before authorizing client execution*) (**Barker, col. 30, lines 56-60**); an identifier of a managed device holding the managed data object; an identifier of an allowed origin managing device; an identifier of an allowed management operation from an allowed origin managing device; and an identifier of an allowed management operation over a holding managed device.

Regarding claim 40, **Barker** discloses the apparatus of claim 37, wherein the third management access template comprises at least one access attribute selected from the group consisting of: an identifier of an allowed management operation (*wherein Each managed object class requires the session identifier as a parameter to each public method. The access permissions associated with the session are examined before authorizing client execution*) (**Barker, col. 30, lines 56-60**); an identifier of a managed data object held on the managed device; an identifier of an allowed origin managing device; an identifier of an allowed management operation from an allowed origin managing device; and an identifier of an allowed management operation over a held managed data object.

Regarding claim 41, **Barker** discloses the apparatus of claim 37, wherein the management verifier component is arranged to determine, from the identifier of a management operation, at least one identifier, the identifier being one selected from the group consisting of: an identifier of a managed data object affected by the operation (*wherein Each managed object class requires the session identifier as a parameter to each public method. The access permissions associated with the session are examined before authorizing client execution*) (**Barker, col. 30, lines 56-60**); and an identifier of a managed device, affected by the operation.

Regarding claim 42, **Barker** discloses the apparatus of claim 37, wherein the management verifier component is arranged to select a management access template, among the first second and third management templates, according to an identifier received in a management order (*wherein the object class IDs received from the management computer are looked up in MIB*) (**Barker, col. 14, lines 43-48**).

Regarding claim 43, **Barker** discloses the apparatus of claim 42, wherein the management verifier component is arranged to select a management access template, among the first second and third management templates, according to an access attribute comprised in another selected management access template (*wherein an instance of an object with the same object class code as another is referenced by calling a lookup function in the application's service object to convert the AP network*

*element instance identifier and application key into its associated instance ID. The combination of these two values in the object identifier uniquely identifies a specific managed object instance) (Barker, col. 14, line 55-col. 15, line 6).*

Regarding claim 44, **Barker** discloses the apparatus of claim 42, wherein the identifier of the origin managing device comprises at least one identifier selected from the group consisting of: an identifier of a management server sending a management order; and an identifier of a user operating the management server (*wherein the client of management computer 26 provides its client ID and port ID, along with a password upon startup and registration) (Barker, col. 30, lines 45-52); and*

*wherein the management verifier component is arranged to select the first management access template according to the at least one identifier (wherein session object ID is given and used to provide access to MIB) (Barker, col. 30, lines 55-58).*

Regarding claim 45, **Barker** discloses the apparatus of claim 42, wherein the identifier of the origin managing device comprises at least one identifier selected from the group consisting of: an identifier of a management server sending a management order; and an identifier of a user operating the management server (*wherein the client of management computer 26 provides its client ID and port ID, along with a password upon startup and registration) (Barker, col. 30, lines 45-52); and wherein the management verifier component is arranged to authenticate the at least one identifier (wherein the client of management computer 26 provides its client ID and port ID, along*

*with a password upon startup and registration) (Barker, col. 30, lines 45-52).*

Regarding claim 46, **Barker** discloses the apparatus of claim 42, wherein the management verifier component is arranged to determine a management role associated to at least one identifier, the identifier being one selected from the group consisting of: an identifier of a management server sending a management order; and an identifier of a user operating the management server (*wherein the client of management computer 26 provides its client ID and port ID, along with a password upon startup and registration) (Barker, col. 30, lines 45-52).*

Regarding claim 47, **Barker** discloses the apparatus of claim 46, wherein the management verifier component is further arranged to select at least one management access template in relationship with the role (*wherein session object ID is given and used to provide access to MIB upon authentication) (Barker, col. 30, lines 55-58).*

Regarding claim 48, **Barker** discloses the apparatus of claim 46, wherein at least one management access template among the second or third management templates comprises an identifier (ROm) of at least one role as an access attribute, and wherein the Management Verifier Component is further arranged to check whether the management order fits with the role (*wherein session object ID is given and used to provide access to MIB. Each command block contains the session ID given at authentication and a command sequence number) (Barker, col. 18, lines 27-53, col.*

**30, lines 55-58).**

Regarding claim 49, **Barker** discloses the apparatus of claim 37, wherein the management verifier component is arranged to determine whether a managed data object affected by an allowed management order is an access attribute in a management access template, and further comprising a management execution component, arranged to execute a management operation over the access attribute (*wherein the network element management server retrieves the client record from local data services and returns the session object to the client noting the client's access permissions. The session object is then used to provide some level of access control in the client application (e.g. deactivating menu element management system for maintenance operations that are not allowed)*) (**Barker, col. 30, lines 45-55**).

Regarding claim 50, **Barker** discloses the apparatus of claim 37, wherein the communication receiver component is further arranged to receive an access request from one of the origin managing devices (*wherein the interface of the element management system server 32 receives management commands from the client 28 of the management computer 26 for the management of the application processor 80/network element 14*) (**Barker, FIG. 1A-1C, and FIG. 2-4 combined, col. 1, line 25-col. 2, line 33**);

wherein the management verifier component is further arranged to determine the first management access template (*wherein session ID of management computer 26 is*

*stored in MIB and looked up in command block of MIB when command is received at network element management system server 32) (Barker, col. 35, line 60-col. 36, line 9); and*

wherein the communication sender component is further arranged to send an access response to the origin managing device that comprises an access attribute of the management access template (*wherein network element management system server 32 responds to management computer 26 with the TRAPs generated to produce responses and acks*) (Black, col. 36, lines 11-24).

Claims 52-61 are corresponding method claims of apparatus claims 41-50; therefore, they rejected under the same rationale.

Claims 63-72 are corresponding computer program claims of apparatus claims 41-50; therefore, they are rejected under the same rationale.

#### ***Response to Arguments***

6. Applicant's arguments, see page 13, filed September 20, 2010, with respect to Rejections of Claims 62-72 under 35 U.S.C. § 101 have been fully considered and are persuasive. The rejections to claims 62-72 as set forth in the previous Office Action have been withdrawn.

***Conclusion***

7. Applicant's arguments as well as request for reconsideration filed on September 20, 2010 have been fully considered but they are moot in view of new ground(s) of rejection.
8. Further references of interest are cited on form PTO-892, which is an attachment to this Office Action.
9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kostas Katsikis whose telephone number is (571)270-5434. The examiner can normally be reached on Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wing Chan can be reached on (571)272-7493. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Wing F. Chan/  
Supervisory Patent Examiner, Art Unit 2441

/Kostas Katsikis/  
Examiner  
Art Unit 2441

November 30, 2010